A Vision for System Safety Enhancement at NASA

Safety Directors' Meeting
Cocoa Beach, Florida,

March 1-5, 2004

Michael Stamatelatos, Ph.D., Director
Safety and Assurance Requirements Division
NASA Office of Safety and Mission Assurance

Deterministic Safety Assessment

- Relies essentially on "established" good engineering practices
- Initiators of accidents are thought of as being essentially hardware related
- Contributions to accidents due to humans and software are ignored
- Focus is on highly adverse consequences only treating them as if they occurred, i.e., without regard to likelihood of occurrence
- Emphasis on deterministic (phenomenological) analyses postulating maximum credible accidents
- Uncertainty and lack of information are dealt with by judgmentally incorporating high safety margins
- Reliability assessment is handled separately from safety and its enhancement is addressed by judgmentally increasing the level of failure tolerance

Drawbacks of Deterministic Safety Assessment

- The focus is on single failure (criticality 1);
- Redundancy (fault tolerance) is arbitrarily prescribed to reduce the chance of failure
- Failure dependencies are not modeled and evaluated
- After a mishap or accident, the safety analysis and improvement effort tends to focus on causes and fixes that are mainly connected with that mishap or accident (fix-run-fix)
- Completeness of all important potential accident scenarios cannot be achieved
- There is no formal way to examine sequences of events, each of which has low consequence, but highly consequential when aggregated into a chain of events (high consequence scenarios)

>>> Experience has shown this situation to be a dominant cause of accidents and mishaps (e.g., Three Mile Island, Bhopal, Challenger, Chernobyl)

Principal Objective of System Safety Is Accident Prevention (NPR 8715.3)

The principal objective of a system safety activity is to provide for an organized, disciplined approach to the early identification and resolution of risks impacting personnel, hardware, or mission success to a level that is as low as reasonably achievable (ALARA).

The system safety activity uses the 6-step risk management approach shown above

What is Risk ?

- **Risk is the measure of the probability and severity of adverse effects.**
  Lowrance, *Of Acceptable Risk*

- **Risk is a set of triplets that answer the questions:**
  1) What can go wrong? (accident scenarios)
  2) How likely is it? (probabilities)
  3) What are the consequences? (adverse effect severity)
  Kaplan & Garrick, *Risk Analysis,* 1981

- **Risk is the combination of: (1) the probability (qualitative or quantitative) that a program or projects will experience an undesired event such as cost overrun, schedule slippage, safety mishap, compromise of security, or failure to achieve a needed technological breakthrough; and (2) the consequences, impact or severity of the undesired event were it to occur.**
  NASA-NPG: 7120.5B

Risk Differs from Hazard

- **Hazard** is the potential for the occurrence of harm or adverse consequence

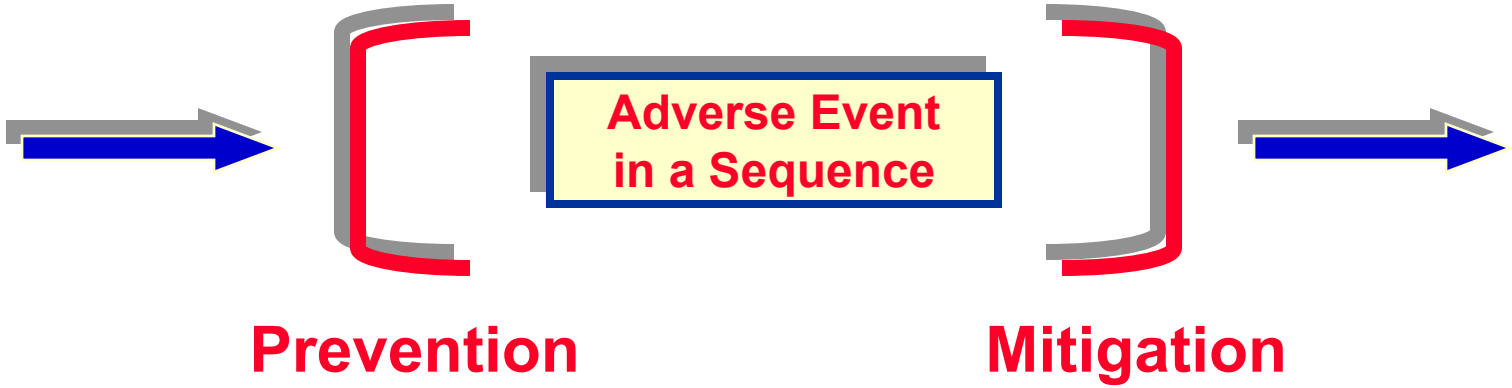
- **Risk** is the **likelihood and severity** of harm or adverse consequence

Examples: space is a hazard but flying into it is a risk

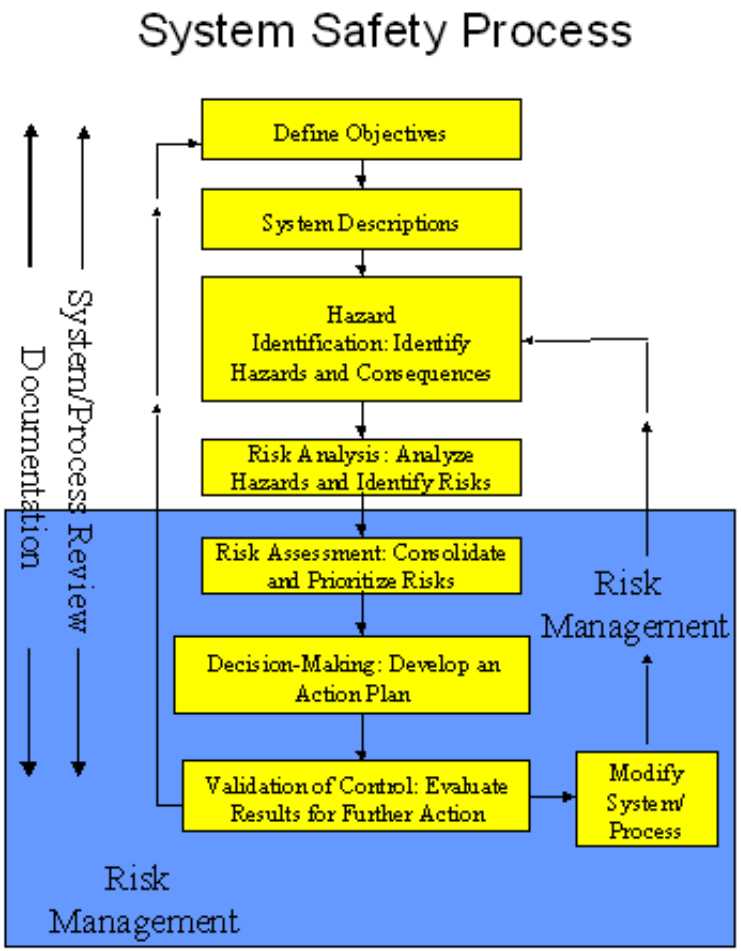
How Does Risk Reduction Work to Improve Safety?

Risk can be reduced through:

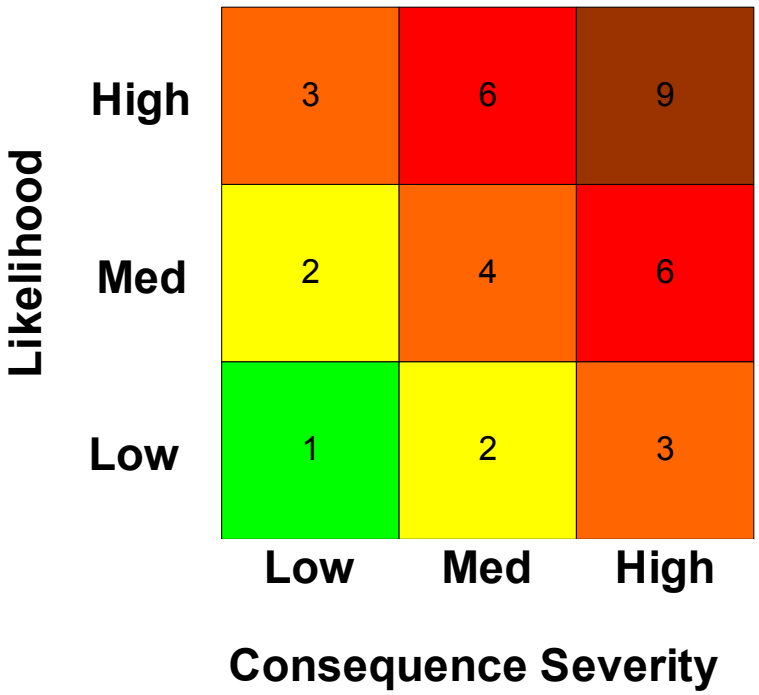
1. **Likelihood Reduction:**
   - Accident or Mishap Prevention (best), or
2. **Severity Reduction:**
   - Accident or Mishap Consequence Mitigation



System Safety Process



Simple Risk Ranking Example

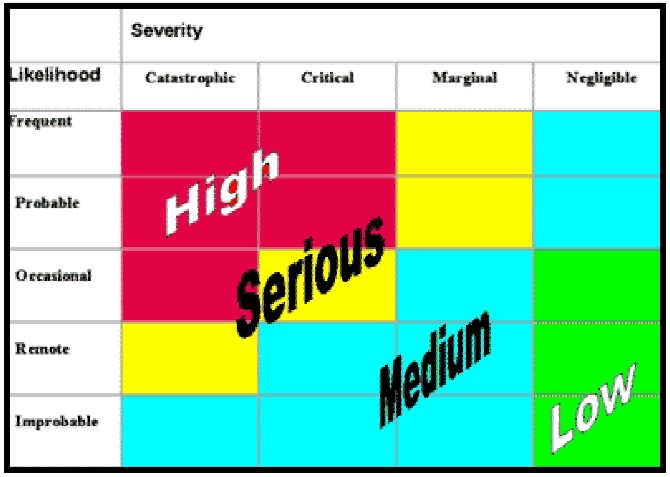


Linguistic variables or category numbers are used for likelihoods and severities

Risk Assessment Matrix (FAA 8040.4)

5 X 4 Matrix

RISK ASSESSMENT MATRIX

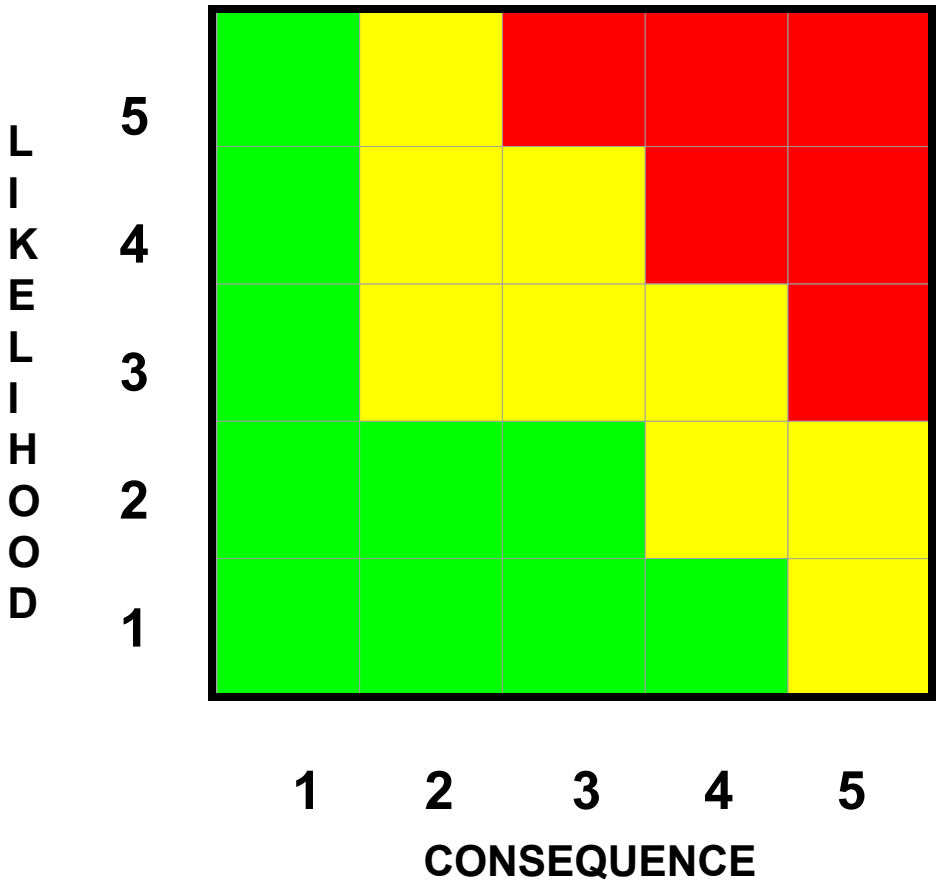


Some of the definitions do not mean the same things to all people

Severity Scale Definitions	
Catastrophic	Results in fatalities and/or loss of the system
Critical	Severe injury and/or major system damage.
Marginal	Minor injury and/or minor system damage.
Negligible	Less than minor injury and/or less than minor system damage.

Likelihood Scale Definitions		
Frequent	Individual	Likely to occur often.
	Fleet	Continuously experienced.
Probable	Individual	Will occur several times.
	Fleet	Will occur often.
Occasional	Individual	Likely to occur some time.
	Fleet	Will occur several times.
Remote	Individual	Unlikely to occur, but possible.
	Fleet	Unlikely but can be expected to occur.
Improbable	Individual	Unlikely; it can be assumed not to occur.
	Fleet	Unlikely to occur, but possible.

NASA Has Used a 5 X 5 Risk Matrix



Legend:

1 – very low
2 – low
3 – moderate
4 – high
5 – very high

Is this matrix better than the previous one?

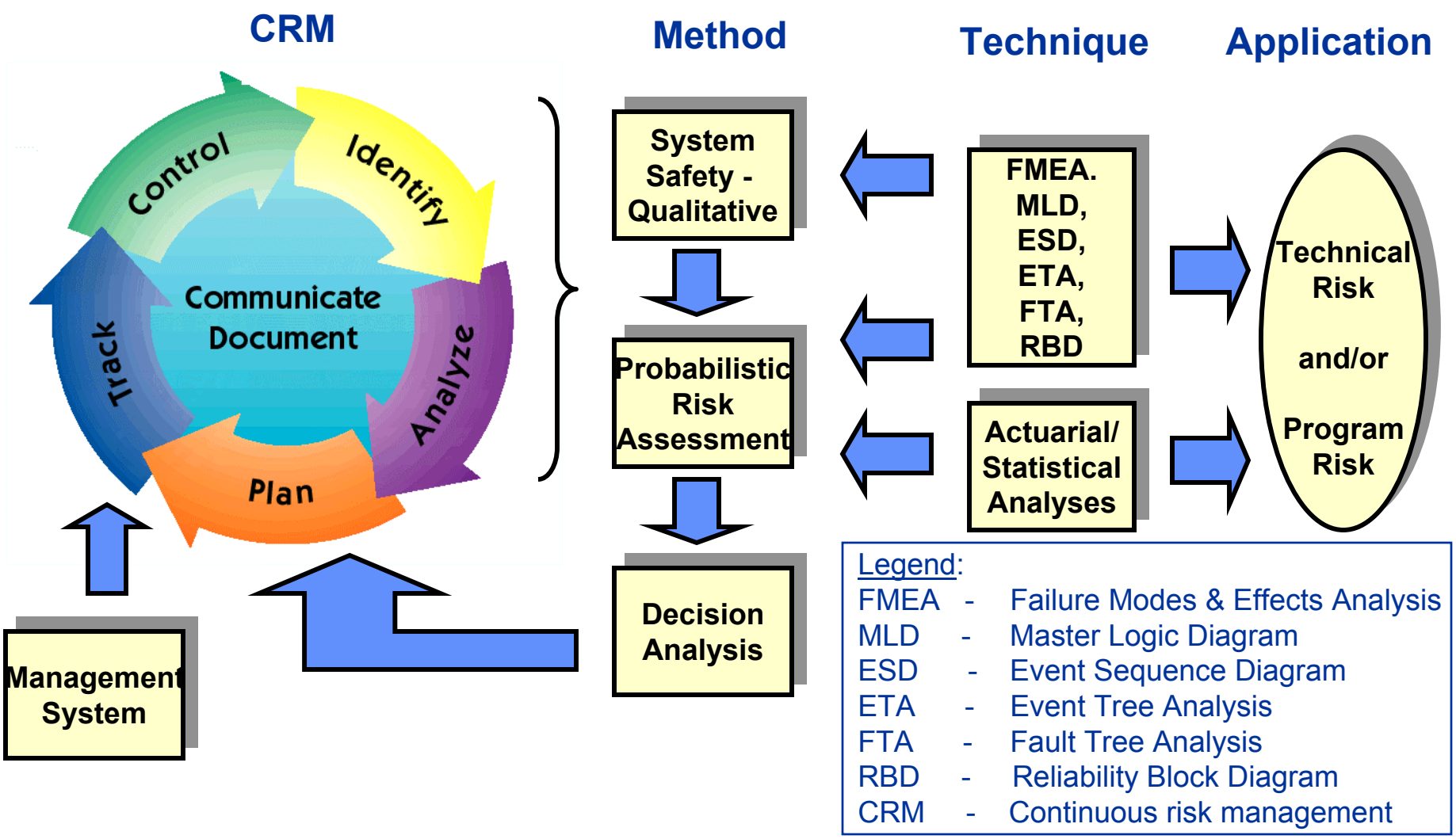
Limitations of the Risk Matrix

- Ambiguity in the severity and likelihood scales may arise
- Without a meaningful scale definition, risks may end up inappropriately lumped up in bins
- Likelihood and severity scales change from project to project in order to best indicate risk differences
- Matrix is unsuitable for combining risks from different projects or programs to show aggregate risk
- Matrix cannot handle more than one risk item at a time
- Matrix cannot properly account for accident scenarios
- Matrix cannot adequately handle dependencies
- Matrix cannot quantify risk and risk priorities
- Uncertainties are not formally accounted for
- Matrix is inadequate to prioritize risk-reduction-driven resource allocation

Decision Making using Traditional System Safety Analysis

- Analysis often uses a "bottom-up" approach. Examples:
  - FMEA: the analyst postulates a failure and assesses its consequences; not good to show risks for other than hardware
  - HAZOP: the analyst postulates a process deviation and assesses its consequences
- Typically one failure or deviation is analyzed at a time.
- Engineering judgment is used to rank risk significance of the postulated failures or deviations.
  - Judgment on how often the hazard can occur
  - Judgment on the severity of the hazard
  - NOTE: Judgment is not quantified (no uncertainty analysis).

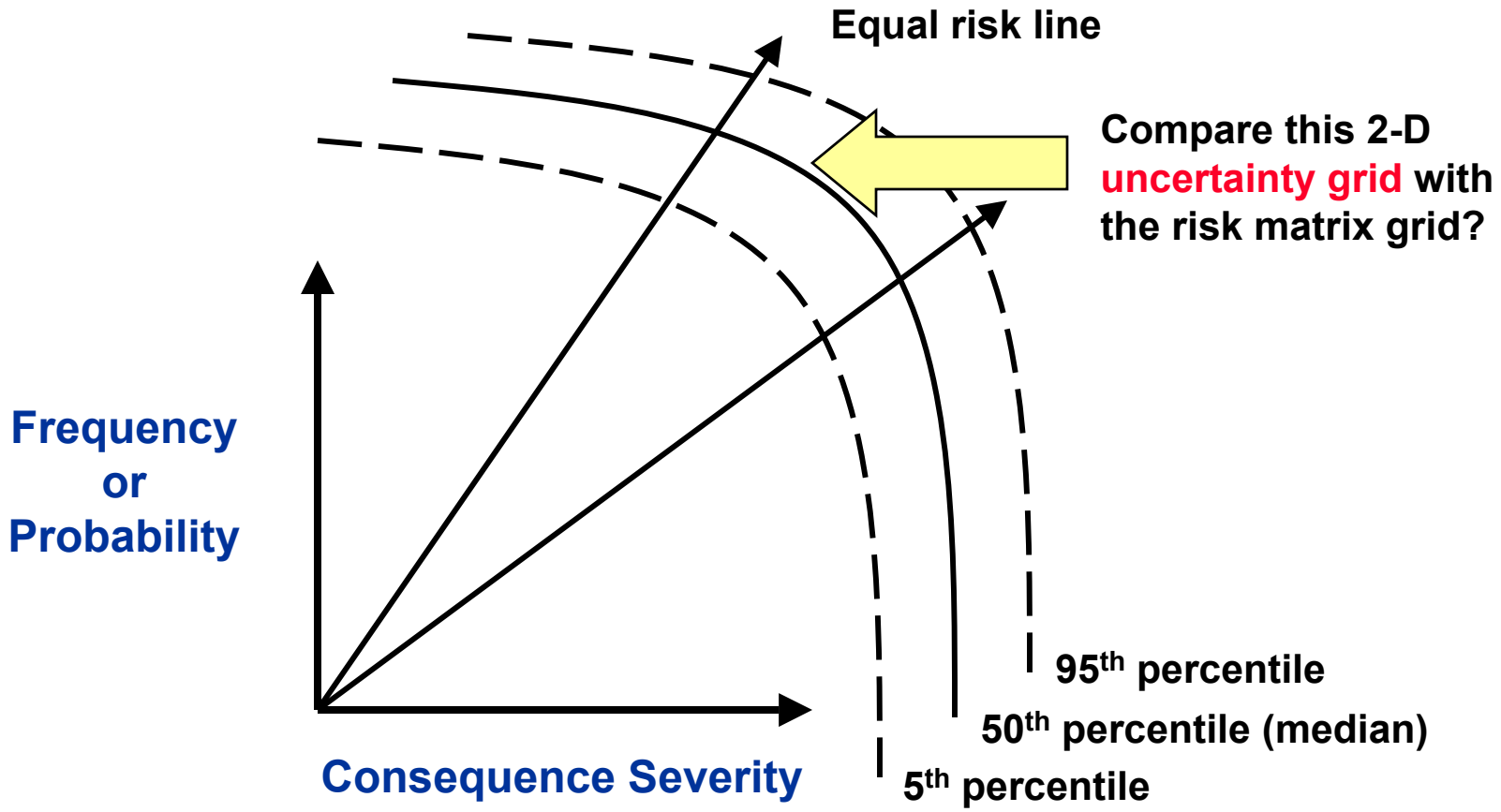
Use of Probabilistic Risk Assessment (PRA) in System Safety



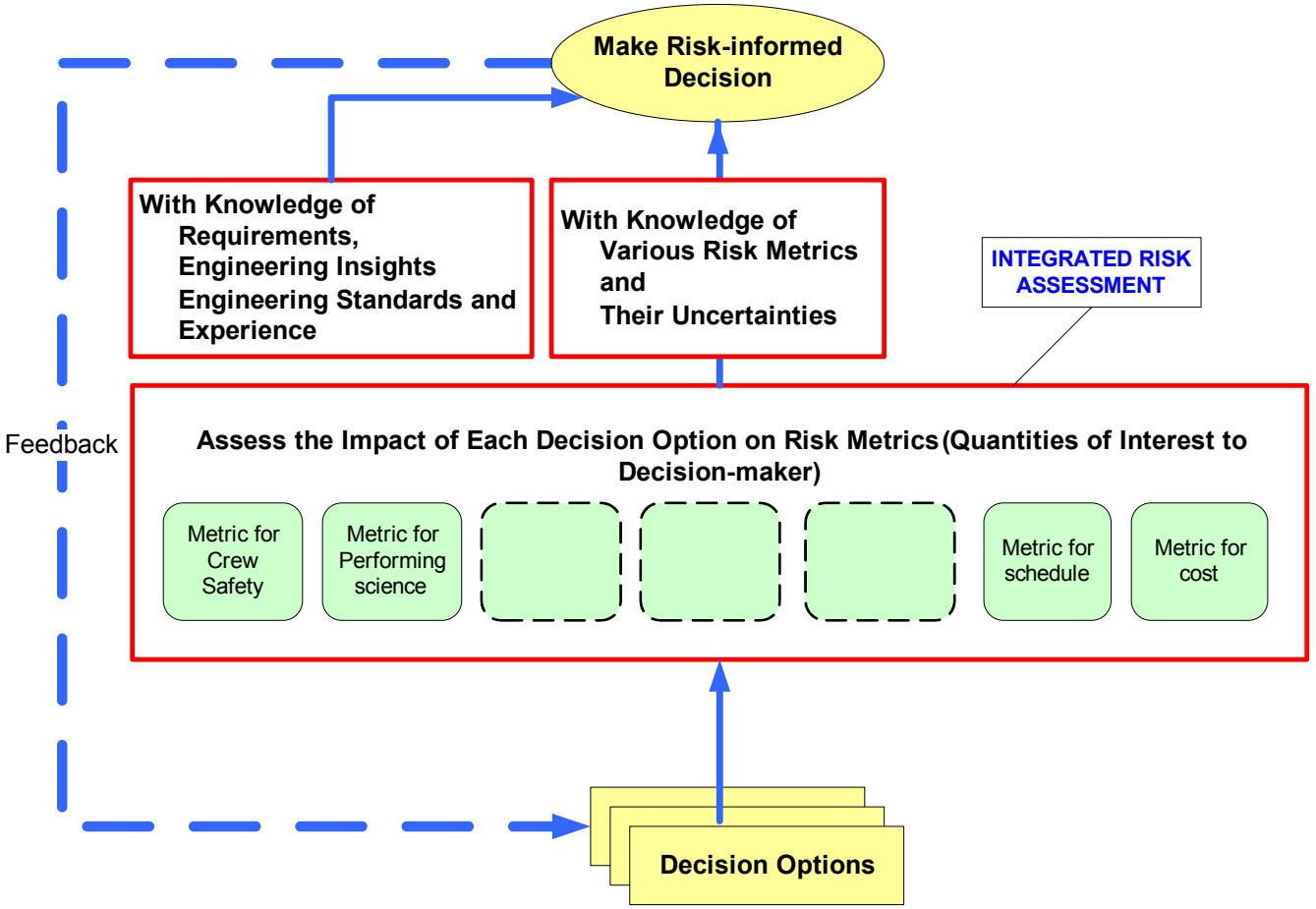
Legend:

FMEA	-	Failure Modes & Effects Analysis
MLD	-	Master Logic Diagram
ESD	-	Event Sequence Diagram
ETA	-	Event Tree Analysis
FTA	-	Fault Tree Analysis
RBD	-	Reliability Block Diagram
CRM	-	Continuous risk management

Quantitative Risk Picture



Elements of Risk-informed Decision Making



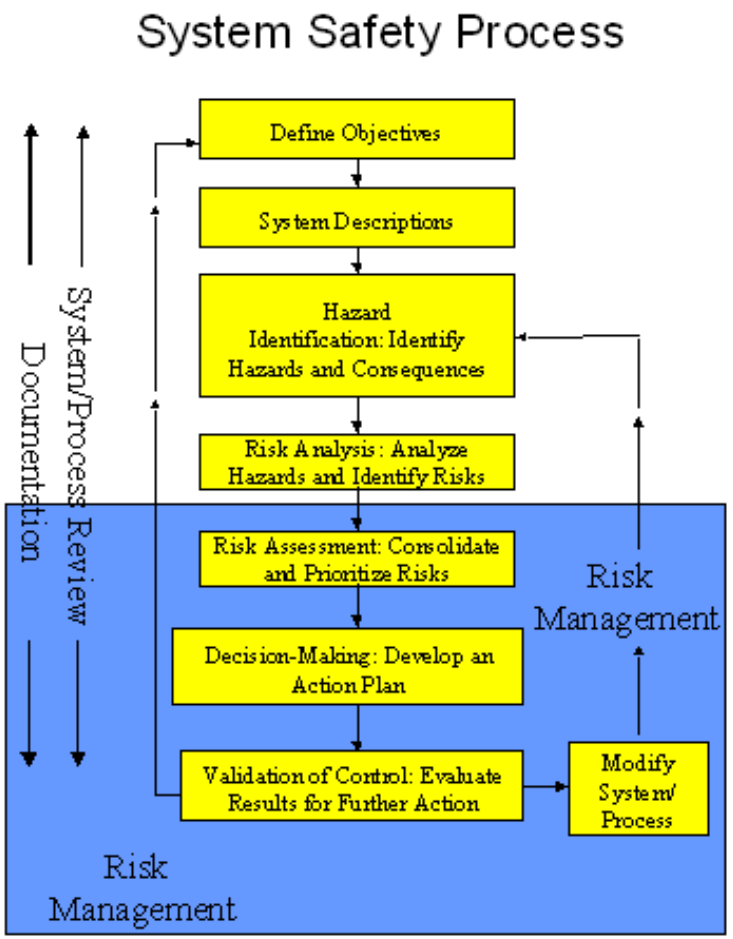
Traditional System Safety Analyses Cannot Support the New Paradigm

- Are not designed to quantify the impact of decision alternatives on any performance measures
  - Cannot quantify any performance metric (e.g., Likelihood of mission success, Likelihood of no crew injury)
- Are not structured to quantify judgments used in the analyses and to quantify uncertainties
  - Cannot provide input to the decision-maker regarding major uncertainties.
  - Cannot advise the decision-maker on whether it is worth investing to reduce certain uncertainties.
- Are not effective to show
  - Compliance with requirements
  - Compliance with engineering standards

Desired Direction of System Safety

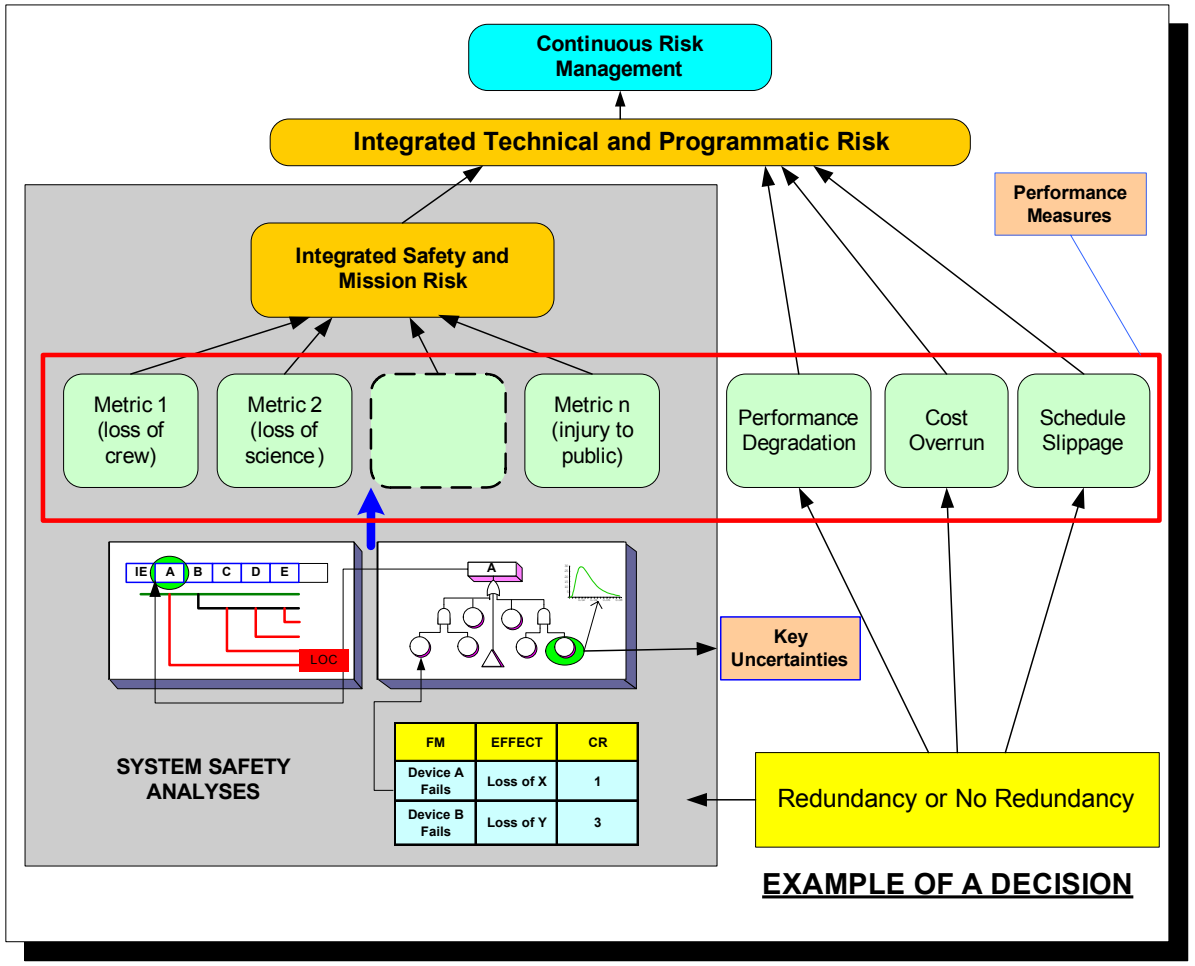
- System safety should drive the Continuous Risk Management (CRM) process both qualitatively and quantitatively
  - Probabilistic risk assessment should be the engine for quantitative assessment of hazards
- Adding the quantitative dimension enhances risk management decision-making:
  - Identifies all credible system failure modes.
  - Captures complex interactions between events/systems/operators
  - Quantifies uncertainties and identifies what the system safety analysts know or do not know
  - Facilitates CRM by identifying the dominant accident scenarios, so that risk management decisions are targeted toward risk significant hazards.
- The key challenge is how to best integrate quantitative risk information with qualitative system safety analysis findings in order to improve the CRM process.

Enhanced System Safety Process



Enhance risk assessment in system safety with a quantitative risk assessment engine

Integration of PRA with Traditional System Safety Analyses



BACKUPS

System Safety Analysis Objectives (Extracted from NPR 8715.3)

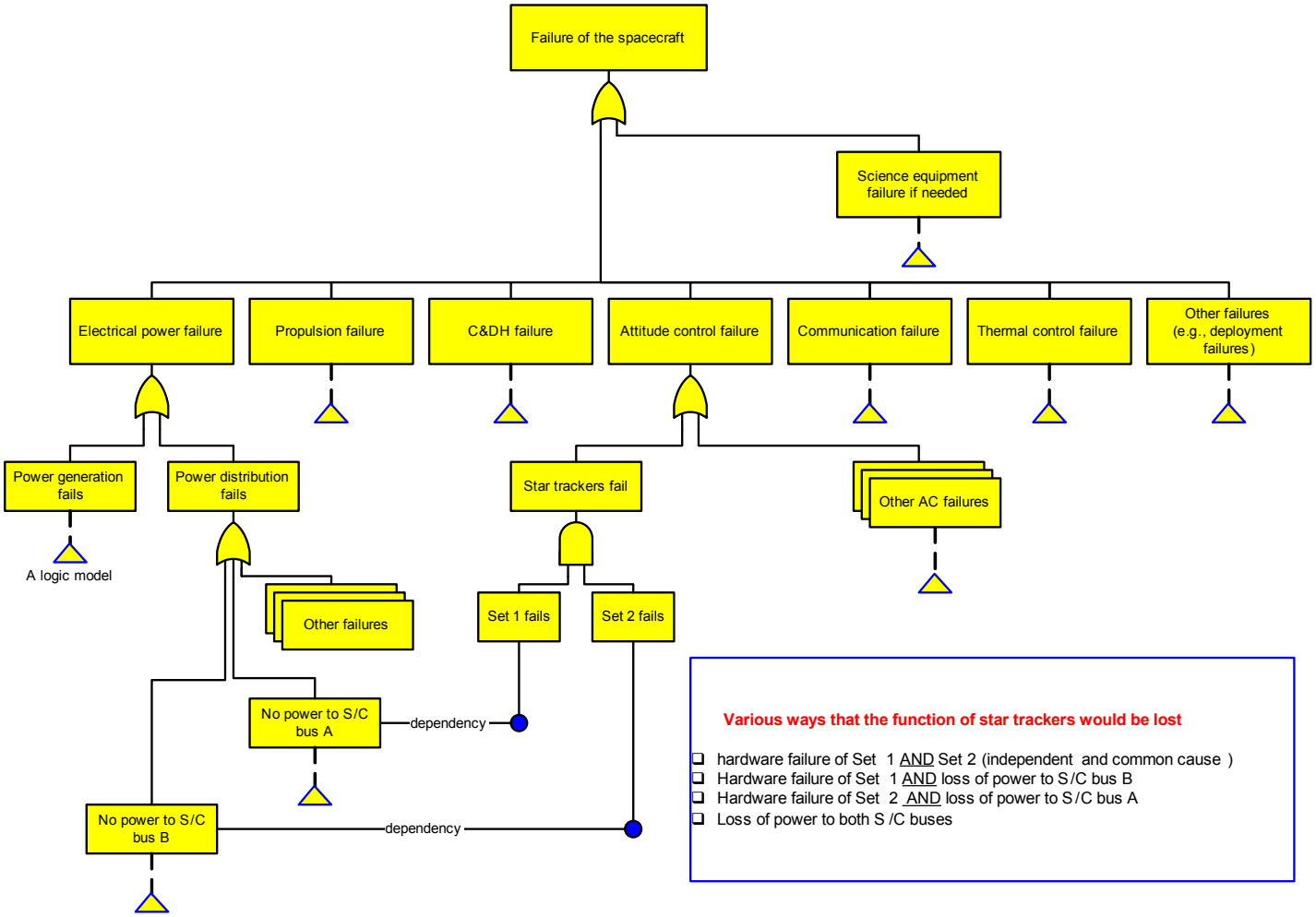
- 3.8.1.1
  - Provides the foundation for the development of safety criteria and requirements.
- 3.8.1.2
  - Determine whether and how the safety criteria and requirements provided to engineering have been included in the design.
- 3.8.1.3
  - Determine whether the safety criteria and requirements created for design and operations have provided an acceptable level of risk for the system.
- 3.8.1.4
  - Provide a roadmap (or methodology) for the development of safety goals and mission success criteria.
- 3.8.1.5
  - Provide a means for demonstrating that safety goals have been met.

System Safety Attempted to Solve These Drawbacks

"The application of engineering and management principles, criteria and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time and cost, throughout all phases of the system cycle"

MIL-STD-882

An Example of Loss of a Critical Function due Systems interactions



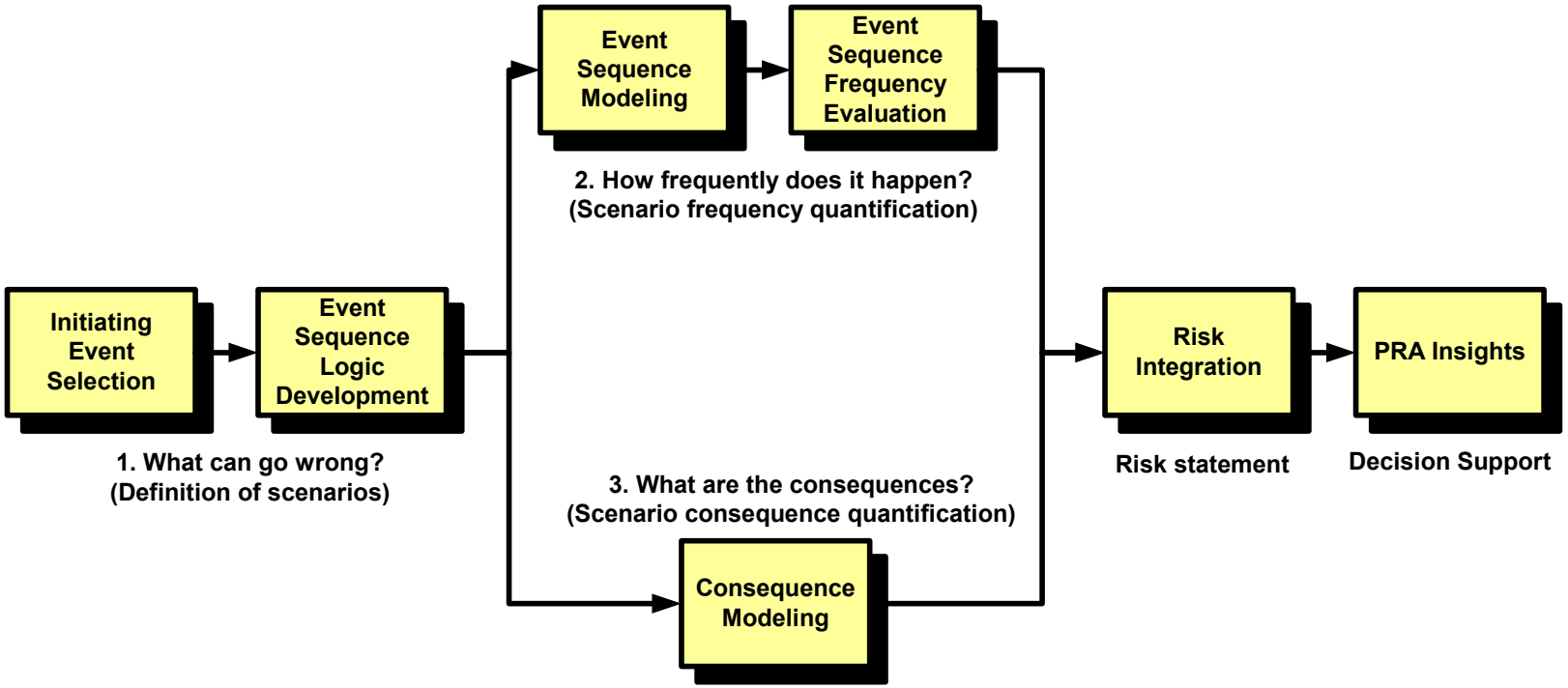
The Concept of Risk Is Introduced

Risk always involves the likelihood that an undesired event will occur.

Risk should consider the severity of consequence of the event, should it occur.

Risk = Likelihood and Severity

PRA Answers Three Basic Questions



PRA is generally used for low-probability and high-consequence events for which insufficient statistical data exist. If enough statistical data exist to quantify system or sub-system failure probabilities, use of some PRA techniques may not be necessary.

Interactive Failures in Complex Systems Lead to Rare Accidents

In his 1984 book "Normal Accidents," Charles Perrow, a Yale sociology professor, states:

- **High-technology undertakings with their highly complex, tightly coupled systems lead to "normal accidents"**
- **Most engineers can identify and counteract single points of weakness or failure in complex systems**
- **Difficulties arise when two or more components in complex systems interact in unexpected ways; these hidden flaws are the so-called "interactive failures."**

Three Mile Island and Mars Polar Lander are both examples of accidents resulting from such interactive failures

This supports the need to incorporate quantitative risk assessment into system safety.

Examples of Needs for System Safety Analyses

- Support the risk management decision-making process
  - Identify and resolve hazards
  - Rank the risk of hazards
  - Propose preventive or mitigation strategies
- Show compliance with deterministic requirements.
  - Is the required level of redundancy met?
- Show compliance with engineering standards.
- Show compliance with program's safety goals (quantitative or qualitative).
  - If quantitative, does the predicted mission success probability meet safety goals?
  - If qualitative, is the impact of the identified hazard as low as reasonably achievable (ALARA)?